Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1 – 28 (canceled).

29. (Currently amended) A method for assisting a user in verifying a cast ballot B_{cast} stored in a server, the method comprising:

forming a digital signature of B_{cast} using a server side private key ~~of the server~~ DS(B_{cast}, s) by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine;

associating the B_{cast} and DS(B_{cast}, s) with a vote serial number VSN by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

forming a confirmation token, comprising DS(B_{cast}, s) and VSN by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

making the confirmation token available by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network;

receiving ~~a~~ the confirmation token made available to ~~a~~ the user by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer hardware machine and executing on the client side physical computer hardware machine via the network;

extracting $VSN_{received\ token}$ and $DS_{received\ token}(B_{cast}, s)$ from the received token by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; ~~and~~

for VSN equal to $VSN_{received\ token}$, comparing $DS_{received\ token}(B_{cast}, s)$ and at least one of $DS(B_{cast}, s)$ and $DS(B_{cast}, S)$ by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; and

~~if the comparison shows equivalence between the data compared,~~ determining that B_{cast} is verified by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if the comparison shows equivalence between the data compared.

30. (Previously presented) The method of Claim 29 wherein:

the confirmation token further comprises a digital signature of an aggregation comprising the associated B_{cast} and VSN using the ~~server's~~ server side private key DS(Aggregation, s);

extracting $DS_{received\ token}$ (Aggregation, s) from the received token; and

B_{cast} is verified only upon the additional condition that $DS_{received\ token}$ (Aggregation, s) is equivalent to DS(Aggregation, s).

31. (Currently amended) A method for assisting a user in verifying a cast ballot recorded in a server, the method comprising:

receiving ~~in~~ by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one set of:

a cast ballot B_{cast} and

a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$;

forming by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine:

a digital signature of B_{cast} using a server side private key ~~of the server~~ $DS(B_{cast}, s)$,

associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN;

forming by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine a confirmation token, comprising:

$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s),

where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN;

making the confirmation token available by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network;

receiving ~~a~~ the confirmation token by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer hardware machine and executing on the client side physical computer hardware machine via the network;

extracting $VSN_{received\ token}$ and at least one of $DS_{received\ token}(B_{cast}, s)$, $DS_{received\ token}(B_{cast}, v)$, and $DS_{received\ token}(AG, s)$ from the received token by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; and

for $VSN_{received\ token}$ and the corresponding VSN, comparing by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one of:

$DS_{received\ token}(B_{cast}, s)$ and $DS(B_{cast}, S)$;

$DS_{received\ token}(B_{cast}, v)$, and $DS(B_{cast}, v)$;

$DS_{\text{received token}}$(Aggregation, s), and DS(Aggregation, s);

~~if comparison shows equivalence between the data compared,~~ determining that B_{cast} is verified by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if comparison shows equivalence between the data compared.

32. (Previously presented) The method of Claim 31 further comprising:

if comparison shows equivalence between $DS_{\text{received token}}$(Aggregation, s), and DS(Aggregation, s), determining that the received confirmation token has not been modified since its formation.

33. (Currently amended) A method for assisting a user verifying a cast ballot recorded in a server, the method comprising:

receiving a cast ballot ("Bcast ") ~~in~~ by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine;

forming a digital signature of Bcast using a server side private key ~~of the server~~ ("DS(Bcast , s)") by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

associating Bcast and DS(Bcast , s) with a vote serial number ("VSN") by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware

machine and executing on the server side physical computer hardware machine; and

for VSN, comparing DS(Bcast , s) and DS(Bcast , S) by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

~~if comparison shows equivalence between the data compared,~~ determining that Bcast is verified by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if the comparison shows equivalence between the data compared.